A brief history of cryptography

Recommend reading: "The Codebreakers" by Kahn

Since the beginning of civilization, there has always been a need to keep secrets. The earliest systematic history of cryptography can be trace back to about 4000 years ago in Egypt.

Between the Egyptians 4000 years ago until the 1960, there has not been much public research into cryptography. The recent surge in interests in cryptography was due to the increase usage of the Internet in 1992.

Between the 1960 and 1990 primarily the military, government and large corporation used cryptographic techniques.

- Feistel's work at IBM in the early 1970 lead to the adoption of DES (Data Encryption Standard) by the US Government into a standard. DES was used to secure non-classified government documents. The US FIPS (United States Federal Information Processing Standard).

- 1976 – Diffie & Hellman published a book titled *"New Direction in Cryptography"*, which gave birth to public-key cryptography.

- 1976 – Rivest, Shamir, Adleman (RSA) discovered the first practical encryption and signature scheme. It was based on the difficulty of factoring large primes.

- 1985 – ElGamal developed a new public-key scheme based on discrete logarithm problem.

- 1991 – International Standard for Digital Signature was adopted (ISO/IEC 9796) based on RSA public-key scheme

- 1994 – The US Government adopted a Digital Signature Standard – DSS, based on ElGamal public-key scheme.

- Present – Advance Encryption Standard (AES – http://www.nist.gov/aes) NIST solicited for an algorithm to replace DES. If all goes as planed, AES will be adopt by Summer 2001 to replace DES.

The distinction between information security and cryptography

Information Security Goal	Cryptography Goal
Confidentiality	**Confidentiality** – via physical or mathematical means
Authorization	
Entity authentication	
Message Authentication	
Data integrity	**Data integrity** – protect data from unauthorized alteration, must be able to detect alteration and manipulation (i.e. insertion, deletion, substitution)
Validation	
Signature	
Access control	
Certification	**Authentication** – applied to the entity and messages.
Time-stamping	
Witnessing	
Receipt	
Non-repudiation	**Non-repudiation**
Ownership	
Anonymity	
Confirmation	
Revocation	

IMHO - The most important concerns of a cryptographer is the prevention and detection of cheating and other malicious activities.

- Criteria for Evaluation of Cryptographic Primitives (Tools)

    1. level of security
    2. functionality
    3. method of operation
    4. performance
    5. **ease of implementation**

Criteria #5 is probably the leading cause of why good cryptographic algorithm is breakable (The most recent example is the DVD encryption scheme that was broken by a 16 years old).

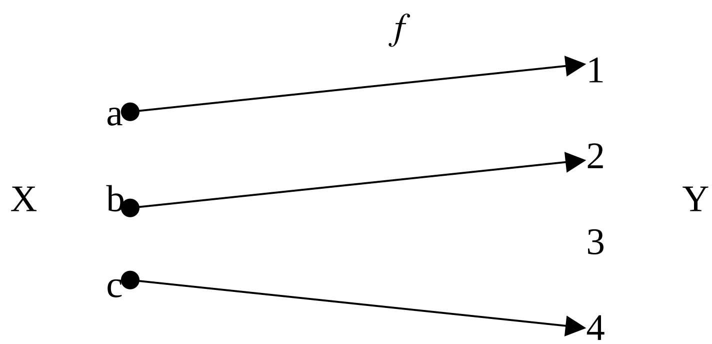
Cryptographic Primitives And Their Inter-relations

<table>
<tr><td rowspan="14">Security primitive</td><td rowspan="3">Unkey primitives</td><td>Arbitrary length hash functions</td><td rowspan="4"></td></tr>
<tr><td>One-way permutation</td></tr>
<tr><td>Random sequences</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="6">Symmetric-key primitives</td><td>Symmetric key cipher</td><td>Block cipher</td></tr>
<tr><td></td><td>Stream Cipher</td></tr>
<tr><td>Arbitraty length hash function (MACs)</td><td rowspan="8"></td></tr>
<tr><td>Signatures</td></tr>
<tr><td>Pseudorandom sequences</td></tr>
<tr><td>Identification primitives</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3">Public-key primitives</td><td>Public-key cipher</td></tr>
<tr><td>Signature</td></tr>
<tr><td>Identification primitives</td></tr>
</table>

The Three Important Functions

1. 1-1 function (transformation)

   A function is 1-1 (one to one) if each of the element in the codomain Y is the image of at most one element in the domain X.

   X = {a, b, c}   Y = {1,2,3,4)

2. One-way function

   f: X → Y is a one way function if $f(x)$ is "easy" to compute for all $x \in$ X but for most elements $y \in$ Im (f) it is "computationally inferasible" to find any $x \in$ X, $\exists f$(x) = y

   i.e. given two large primes, p and q, it is quite easy to computer n=pq. but the reverse is not true,

   given n

   it is quite difficult to find p and q, especially if n is a large number.

3. Trap-door one-way function

   f: X → Y with certain 'secret information' it is quite easy to compute y $\in$ Im(f), and $x \in$ X, $\exists f$(x) = y

   i.e. given n = pq if you know either (n,p) or (n,q) it is quite easy to get the component factor of n separately (p,q).

Some Common Key Letters and Terminology

Encryption domains and codomains

- A denotes a finite set called the *alphabet definition*. i.e. $A = \{0,1\}$, the *binary alphabet*

- M denotes a set called *message space*. M consists of all strings of symbols from the *alphabet definition*. An element of M is the *plaintext message* or simply the *plaintext.*

- C denotes a set called the *cipher space*. An element of C is called the *ciphertext*.

Encryption and decryption transformations

- K denotes a set called the *key space*. An element of K is called a *key*.

- Each element $e \in K$ uniquely determine a bijection from M to C, denoted by E_e . E_e called an *encryption function* or *encryption transformation*. E_e must be bijection if the process is to be reverse, in general:

  Define E_e as a 1-1 transformation from M to C. E_e is a bijection from M to $\mathrm{Im}(E_e)$ where $\mathrm{Im}(E_e)$ is a subset of C.

- For each $d \in K$, D_d denotes a bijection from C to M (i.e. $D_d : C \rightarrow M$). D_d is called a *decryption function* or *decryption transformation*.

- ***Encryption of*** m: The process of applying transforming E_e to a message $m \in M$.

- ***Decryption of*** c: The process of applying transformation D_d to the ciphertext c.

- *Encryption scheme* (cipher) consists of a set:

  $\{E_e : e \in K\}$ - encryption transformation
  $\{D_d : d \in K\}$ – decryption transformation

Having the following property:

$e \in K$ the is a unique key $d \in K$ such that $(\exists)$ $D_d = E_e^{-1}$; that is,

$D_d\,(E_e(m)) = m$ for all $m \in M$

- e and d (e,d) are key pair. *Can e and d be the same?*

Summary: To construct an encryption scheme require the following:

1. Select a message space M
2. A cipher space C
3. A key space K
4. A set of encryption and decryption transformation: $\{E_e : e \in K\}$ and $\{D_d : d \in K\}$.

Example: Shift Cipher (pg. 4, figure 1.2)

Let $M = C = K = Z_{26}$. For $0 \le K \le 25$, we define the following

$$e_K(x) = x + K \bmod 26$$

$$d_K(y) = y - K \bmod 26$$

where (x,y) are element of Z_{26} $(x,y \in Z_{26})$.

A	0		N	13
B	1		O	14
C	2		P	15
D	3		Q	16
E	4		R	17
F	5		S	18
G	6		T	19
H	7		U	20
I	8		V	21
J	9		W	22
K	10		X	23
L	11		Y	24
M	12		Z	25

Using the table on the left with $K = 15$, decrypt the following message:

I W T H C D L X H Q T N J I X U J A

Example: Substitution Cipher (pg. 7, figure 1.3)

Let $M = C = K = Z_{26}$. K consists of all possible permutation of 26 symbols 0, 1, …., 25. For each $\pi \in K$, we define the following:

$$e_\pi(x) = \pi(x)$$

$$d_\pi(y) = \pi^{-1}(y)$$

where π^{-1} is the inverse permutation of π.

a	X		n	S
b	N		o	F
c	Y		p	L
d	A		q	R
e	H		r	C
f	P		s	V
g	O		t	M
h	G		u	U
i	Z		v	E
j	Q		w	K
k	W		x	J
l	B		y	D
m	T		z	I

Using the table on the left decrypt the following message:

MGHVSFKZVNHXUMZPUB

Example: Affine Cipher (pg. 11, figure 1.4)

Let $M = C = K = Z_{26}$. and let

$$K = \{(a,b) \in Z_{26} \times Z_{26} : \gcd(a,26) = 1\}$$

For K' = $(a,b) \in K$, we define the following:

$$e_{K'}(x) = ax + b \bmod 26$$

$$d_{K'}(y) = a^{-1}(y - b) \bmod 26$$

$(x,y \in Z_{26})$.

<u>*Example 1.3, Pg. 11*</u>

K' = (7,3)

$e_{K'}(x) = 7x + 3$

$d_{K'}(y) = 15y - 19$

Typical Communication Channels and Risks